WHAT IS CLAIMED IS:

1. A bi-directional communications system integrated with a remote web-based expert data center wherein a medical programmer for an IMD is uplinked to the web-based expert data center via the bi-directional communications system, the web-based expert data center in configuration with the programmer forming a secure medical information exchange network wherein patient records are transferred, the medical information exchange network comprising:

a database residing within the programmer for storing sensitive information;

a key source in data communications with the programmer and the web-based expert data center for transmitting an encryption key to the programmer and a decryption key to the expert-data center;

an encryption engine residing within the programmer for encrypting the sensitive information using the encryption key;

an interface for coupling the programmer to the expert data center; and

a decryption engine residing within the expert data center for decrypting the encrypted sensitive information using the decryption key.

2. The system of claim 1, wherein the programmer device is in telemetric communication with the implantable medical device.

3. The system of claim 2, wherein the sensitive information stored within the database includes data obtained from the implantable medical device.

4. The system of claim 1, wherein the sensitive information stored within the database includes confidential patient information.

5. The system of claim 1, wherein the interface is a telephone line connection.

6. The system of claim 1, wherein the interface is an intranet connection.

7. The system of claim 1, wherein the interface is an internet connection.

8. The system of claim 1, wherein the interface is a satellite connection.

9. The system of claim 1, wherein the interface is a global positioning system connection.

10. The system of claim 1, wherein the interface comprises at least two communication links selected from the group of communication links consisting of a telephone line communication, an intranet communication, an internet communication, a satellite communication, and a global positioning system communication.

11. The system of claim 1, wherein the encryption key and the decryption key are symmetric keys.

12. The system of claim 1, wherein the encryption key and the decryption key are asymmetric keys.

13. The system of claim 1, wherein the encrypted sensitive information includes a digital signature.

14. The system of claim 1, wherein the remote expert data center is a second medical device.

15. A bi-directional communications system integrated with a remote web-based expert data center wherein a medical programmer for an IMD is uplinked to the web-based expert data center via the bi-directional communications system, the web-based expert data center in configuration with the programmer forming a secure medical information exchange network wherein patient records are transferred, the medical information exchange network comprising a system for transferring information from a to a programmer, the system comprising:

a database residing within the remote expert data center for storing sensitive information;

a key source in data communications with the programmer and the remote expert data center for distributing an encryption key to the remote expert data center and a decryption key to the programmer;

an encryption engine residing within the remote expert data center for encrypting the sensitive information using the encryption key;

an interface for coupling the remote expert data center to the programmer; and

a decryption engine residing within the programmer for decrypting the encrypted sensitive information using the decryption key.

16. The system of claim 15, wherein the programmer is in telemetric communications with an implantable medical device in a patient.

17. The system of claim 16, wherein the sensitive information stored within the database includes data obtained from the implantable medical device.

18. The system of claim 15, wherein the sensitive information stored within the database includes confidential patient information.

19. The system of claim 15, wherein the interface is a telephone line connection.

20. The system of claim 15, wherein the interface is an intranet connection.

21. The system of claim 15, wherein the interface is an internet connection.

22. The system of claim 15, wherein the interface is a satellite connection.

23. The system of claim 15, wherein the interface is a global positioning system connection.

24. The system of claim 15, wherein the interface consists at least one communication link selected from the group of communication links consisting of a telephone line communication, an intranet communication, an internet communication, a satellite communication, and a global positioning system communication.

25. The system of claim 15, wherein the encryption key and the decryption key are symmetric keys.

26. The system of claim 15, wherein the encryption key and the decryption key are asymmetric keys.

27. The system of claim 15, wherein the encrypted sensitive information includes a digital signature.

28. A system for transferring information between a programmer and a remote expert data center, the system comprising:

a key source in data communications with the programmer and the remote expert data center for distributing a set of encryption keys to the programmer and the remote expert data center;

an interface for coupling the programmer to the remote expert data center;

a first encryption engine residing within the programmer for encrypting a first set of sensitive information residing in the programmer using one of the set of encryption keys generated by the key source;

a second encryption engine residing within the remote expert data center for encrypting a second set of sensitive information residing in the remote expert data center using one of the set of encryption keys generated by the key source;

a first decryption engine residing within the programmer for decrypting the second set of sensitive information generated by the second encryption engine; and

a second decryption engine residing within the remote expert data center for decrypting the first set of sensitive information generated by the first encryption engine.

29. The system of claim 28, wherein the programmer is in electrical communication with an implantable medical device in a patient.

30. The system of claim 29, wherein the first set of sensitive information includes data obtained from the implantable medical device.

31. The system of claim 28, wherein the first set of sensitive information includes confidential patient information.

32. The system of claim 28, wherein the interface is a telephone line connection.

33. The system of claim 28, wherein the interface is an intranet connection.

34. The system of claim 28, wherein the interface is an internet connection.

35. The system of claim 28, wherein the interface is a satellite connection.

36. The system of claim 28, wherein the interface is a global positioning system connection.

37. The system of claim 28, wherein the interface comprises at least one communication link selected from the group of communication links consisting of a telephone line communication, an intranet communication, an internet communication, a satellite communication, and a global positioning system communication.

38. The system of claim 28, wherein the set of encryption keys are symmetric keys.

39. The system of claim 28, wherein the set of encryption keys are asymmetric keys.

40. The system of claim 28, wherein the first set of sensitive information includes a digital signature.

41. The system of claim 28, wherein the second set of sensitive information includes a digital signature.

42. A system for securely transferring sensitive information received from at least one lead positioned within a passageway of a heart related to an implantable medical device to a remote expert data center, the system comprising:

a programmer in data communication with the implantable medical device for receiving and processing the sensitive information from the implantable medical device;

a key source in data communication with the programmer and the remote expert data center for distributing an encryption key to the programmer and a decryption key to the remote expert data center;

an encryption engine residing within the programmer for encrypting the sensitive information using the encryption key;

an interface for coupling the programmer to a remote expert data center; and

a decryption engine residing within the remote expert data center for decrypting the encrypted sensitive information using the decryption key.

43. The system of claim 42, wherein the interface is a telephone line connection.

44. The system of claim 42, wherein the interface is an intranet connection.

45. The system of claim 42, wherein the interface is an internet connection.

46. The system of claim 42, wherein the interface is a satellite connection.

47. The system of claim 42, wherein the interface is a global positioning system connection.

48. The system of claim 42, wherein the interface consists of at least one communication link selected from the group of communication links consisting of a telephone line communication, an intranet communication, an internet communication, a satellite communication, and a global positioning system communication.

49. The system of claim 42, wherein the encryption key and the decryption key are symmetric keys.

50. The system of claim 42, wherein the encryption key and the decryption key are asymmetric keys.

51. The system of claim 42, wherein the encrypted sensitive information includes a digital signature.

52. A method of securely transferring sensitive information from a programmer to a remote expert data center, the method comprising:

generating an encryption key for distribution to the programmer;

generating a decryption key for distribution to the remote expert data center;

encrypting the sensitive information residing on the programmer with the encryption key;

transferring the encrypted sensitive information from the programmer to the remote expert data center; and

decrypting the encrypted sensitive information residing on the remote expert data center with the decryption key.

53. The method of claim 52, wherein the programmer is connected to an implantable medical device in a patient.

54. The method of claim 52, wherein the step of encrypting the sensitive information residing on the programmer further comprises:

creating a digital signature for the encrypted sensitive information.

55. The method of claim 54, wherein the step of decrypting the encrypted sensitive information residing on the remote expert data center further comprises:

verifying the digital signature associated with the encrypted sensitive information.

56. A method of securely transferring sensitive information from a remote expert data center to a programmer, the method comprising:

generating an encryption key for distribution to the remote expert data center;

generating a decryption key for distribution to the programmer;

encrypting the sensitive information residing on the remote expert data center with the encryption key;

transferring the encrypted sensitive information from the remote expert data center to the programmer; and

decrypting the encrypted sensitive information residing on the programmer with the decryption key.

57. The method of claim 56, wherein the programmer is connected to an implantable medical device in a patient.

58. The method of claim 56, wherein the step of encrypting the sensitive information residing on the remote expert data center further comprises:

creating a digital signature for the encrypted sensitive information.

59. The method of claim 58, wherein the step of decrypting the encrypted sensitive information residing on the programmer further comprises:

verifying the digital signature associated with the encrypted sensitive information.

60. A system for transferring information from a programmer to a remote expert data center, the system comprising:

means for generating an encryption key for distribution to the programmer;

means for generating a decryption key for distribution to the remote expert data center;

means for encrypting the sensitive information residing on the programmer with the encryption key;

means for transferring the encrypted sensitive information from the programmer to the remote expert data center; and

means for decrypting the encrypting sensitive information residing on the remote expert data center with the decryption key.

61. The method of claim 60, wherein the programmer is connected to an implantable medical device in a patient.

62. The system of claim 60, wherein the means for encrypting the sensitive information residing on the programmer further comprises:

means for creating a digital signature for the encrypted sensitive information.

63. The system of claim 62, wherein the means for decrypting the encrypted sensitive information residing on the remote expert data center further comprises:

means for verifying the digital signature associated with the encrypted sensitive information.

64. A system for transferring sensitive information from a remote expert data center to a programmer, the system comprising:

means for generating an encryption key for distribution to the remote expert data center;

means for generating a decryption key for distribution to the programmer;

means for encrypting the sensitive information residing on the remote expert data center with the encryption key;

means for transferring the encrypted sensitive information from the remote expert data center to the programmer; and

means for decrypting the encrypting sensitive information residing on the programmer with the decryption key.

65. The system of claim 64, wherein the programmer is connected to an implantable medical device in a patient.

66. The system of claim 64, wherein the means for encrypting the sensitive information residing on the remote expert data center further comprises:

means for creating a digital signature for the encrypted sensitive information.

67. The system of claim 66, wherein the means for decrypting the encrypted sensitive information residing on the programmer further comprises:

means for verifying the digital signature associated with the encrypted sensitive information.

68. A remote expert data center readable medium containing instructions for controlling a remote expert data center system to perform a method for securely transferring sensitive information from a programmer to a remote expert data center, the method comprising:

generating an encryption key for distribution to the programmer;

generating a decryption key for distribution to the remote expert data center;

encrypting the sensitive information residing on the programmer with the encryption key;

transferring the encrypted sensitive information from the programmer to the remote expert data center; and

decrypting the encrypted sensitive information residing on the remote expert data center with the decryption key.

69. A remote expert data center readable medium containing instructions for controlling a remote expert data center system to perform a method for securely transferring sensitive information from a remote expert data center to a programmer, the method comprising:

generating an encryption key for distribution to the remote expert data center;

generating a decryption key for distribution to the programmer;

encrypting the sensitive information residing on the remote expert data center with the encryption key;

transferring the encrypted sensitive information from the remote expert data center to the programmer; and

decrypting the encrypted sensitive information residing on the programmer with the decryption key.

5